IP Address Geolocation

https://campus.barracuda.com/doc/92767303/

To restrict traffic from geographic regions or certain categories of traffic, Barracuda WAF-as-a-Service provides an IP filter that can be applied to an entire geographic region or collection of regions spanning multiple countries and/or continents.

Traffic from the selected geographic regions and source categories is blocked at the Barracuda WAF-as-a-Service proxy and will not reach the back-end server. You can configure an exception list of IP subnets to override the IP filter and allow certain traffic, even if it originates from a blocked source.

Set **IP Address Geolocation** to **ON** to allow or block access to your application based on user's location and specific categories of IPs.

Geo IP Filter

Select the geographical regions from where access to your application can be allowed or blocked. By default, Barracuda WAF-as-a-Service allows access to IP addresses from all geographical regions listed under the **Allowed** section. To block IP addresses from specific regions, select the geographical region(s) under **Allowed** and click the single angle bracket. IP addresses from the selected geographical regions will be blocked from accessing your application.

IP Categories

Select the categories of IP Addresses that you want to block from accessing your application. The IP categories that are available are:

- **Barracuda Reputation Blocklist** - IP addresses that are identified as potential originators of spam, malware, and bots.
- **TOR Nodes** - IP addresses that are identified as TOR.
- **Anonymous Proxy** - IP address is from an anonymizer that hides the IP address of the requesting client.
- **Satellite Provider**- IP address is from a Satellite Internet Service Provider (ISP) so the IP address of the requesting client is unknown.
- **Unrecognized IPs**- unrecognized Public/Private IP addresses
- **Known HTTP Attack Sources** - IP addresses that scan HTTP/HTTPS requests for vulnerable installations of known web applications and brute force logins.
- **Known SSH Attack Sources** - IP addresses that run attacks on the service SSH.
- **Datacenter IPs** - IP address is from a range of data centers and is therefore not the user but

rather a program.
- **Fake Crawler** - IP addresses of robots that crawl the web application by sending user-agent strings of reputed/popular search engines such as Google, Bing, Yandex, etc.

When set to **Block**, all requests from the selected categories will be terminated and logged. By default, all categories are set to **Allow**.

IPs to Always Allow

Use this section to configure the IP address(es) and associated subnet mask that needs to be allowed even though the IP address is from the blocked geographical region specified in the **Geo IP Filter**, or **IP Categories**.

IPs to Always Block

Use this section to configure the IP address(es) and associated subnet mask that needs to be blocked even though the IP address is from the allowed geographical region specified in the **Geo IP Filter**, or **IP Categories**.